International Journal of Cybersecurity Intelligence & Cybercrime

Volume 4 | Issue 2 Article 3

8-2021

Malware Infections in the U.S. during the COVID-19 Pandemic: An Empirical Study

COVID-19; malware infection; closed non-essential businesses; closed K-12 schools

Follow this and additional works at: https://vc.bridgew.edu/ijcic

Part of the Criminology Commons, Criminology and Criminal Justice Commons, Forensic Science and Technology Commons, and the Information Security Commons

Recommended Citation

Gero, S. L., Back, S., LaPrade, J., & Kim, J. (2021). An empirical study on cybercrime and COVID-19. International Journal of Cybersecurity Intelligence and Cybercrime, 4(2), 25-37. https://www.doi.org/10.52306/04020321CRBH5596

This item is available as part of Virtual Commons, the open-access institutional repository of Bridgewater State University, Bridgewater, Massachusetts.
Copyright © 8-2021 Sydney Gero, Sinchul Back, Jennifer LaPrade, and Joonggon Kim

Gero et al. (2021). *International Journal of Cybersecurity Intelligence and Cybercrime, 4*(2), 25-37.

Malware Infections in the U.S. during the COVID-19 Pandemic: An Empirical Study

Sydney Gero*, The University of Scranton, U.S.A.
Sinchul Back, The University of Scranton, U.S.A.
Jennifer LaPrade, Missouri State University, U.S.A.
Joonggon Kim, Keimyung University, South Korea

Keywords: COVID-19; malware infection; closed non-essential businesses; closed K-12 schools

Abstract:
The COVID-19 pandemic has changed the world in many ways, especially in the landscape of cyber threats. The pandemic has provided cybercriminals with more opportunities to commit crimes due to more people engaging in online activities, along with the increased use of computers for school, work, and social events. The current study seeks to explore cybercrime trends, in particular malware infections, during the COVID-19 pandemic. Thus, this study examines the relationship between the number of malware infections, COVID-19 positive cases, closed non-essential businesses, and closed K-12 public schools in the United States. Data utilized in this study derives from (1) Kaspersky Cyberthreat Real-Time Map, (2) Centers for Disease Control and Prevention (CDC), and (3) COVID-19 US State Policy Database over the course of six months from January of 2020 to June of 2020. The findings of this study reveal that there are associations between the number of malware infections, COVID-19 positive cases, and closed non-essential businesses. However, interestingly, there is no link between the number of malware infections and closed K-12 public schools. Policy implications and the limitations of this study are also discussed.

Introduction

The nature of the COVID-19 pandemic is unprecedented. The virus resulted in new policies and practices (i.e., masks and social distancing) across the United States, which changed the way we live. Advances in cyberspace and technology also transformed our daily lives. For example, the convenience of e-mails and text messages radically altered how we communicate with one another. The growing use of computers, tablets, and smartphones made communication easier and faster. However, technology created an emerging field of crime: cybercrime. Information technology and interconnectivity facilitate cybercriminals to utilize the internet to exploit online users. Given that, it can provide more criminal opportunities.

As society becomes increasingly more reliant on technology, the prevalence of cybercrime will only continue. The onset of the COVID-19 pandemic in the U.S. during the early months of 2020 then intensified society's dependence on technology through the nationwide lockdowns and mandatory stay-at-home orders that caused non-essential businesses and K-12 public schools to close. As a result, work, school, and social gatherings switched to cyberspace. Although employed individuals may have had some experience with teleworking, most workers had no choice but to quickly learn and use cyberspace to continue their work life. For example, work meetings were instead completed over the phone or video chat rather than in a conference room. From February to May of 2020, nearly half of American workers were working remotely (Brynjolfsson et al., 2020).

*Corresponding author
Sydney Gero, Sociology, Criminal Justice And Criminology Department, 800 Linden St., O'Hara Hall Room, Scranton, PA, 18510, U.S.A.
Email: sydney.gero@scranton.edu

Reproduction, posting, transmission or other distribution or use of the article or any material therein, in any medium as permitted by written agreement of the International Journal of Cybersecurity Intelligence and Cybercrime, requires credit to the Journal as follows: "This Article originally appeared in International Journal of Cybersecurity Intelligence and Cybercrime (IJCIC), 2021 Vol. 4, Iss. 2, pp. 25-37" and notify the Journal of such publication.
© 2021 IJCIC 2578-3289/2021/08

Students and teachers faced the same dilemma, as school classrooms were converted into virtual classrooms. The difficulty in holding the attention of elementary school children only escalated through a computer screen. Moreover, the school classrooms that formerly prohibited phones and technology now depended entirely on it. The average person's lifestyle ultimately changed, while also increasing their exposure to cybercriminals and their deviant acts.

In the U.S., cybercrime victimization steadily increased over the past several years. In 2015, nearly 300,000 cybercrime complaints were filed, accumulating to a little over $1 billion in victim losses (Internet Crime Report, 2019). Later in 2019, over 400,000 complaints were filed, and victim losses amounted to $3.5 billion (Internet Crime Report, 2019). The present study will focus on malware infections, one type of cybercrime, which are viruses consisting of malicious software used to disrupt services or extract data (Lallie et al., 2020). In 2019, over 2,000 victims reported malware infections, which amounted to over $2 million in losses (Internet Crime Report, 2019). While some malware infections are easily recognizable, many can go undetected and thus unreported. Therefore, malware infections pose a large threat to frequent Internet users, making this type of cybercrime the focus of the current study.

More importantly, no study has empirically examined the relationship between the COVID-19 pandemic and cybercrime victimization, focusing on malware infections in the United States. We believe societal changes as a result of the COVID-19 pandemic, dramatically altered cybercrime. Thus, this study empirically investigates the relationship between malware infections, COVID-19 reported positive cases, closed non-essential businesses, and closed K-12 public schools from January 2020 to June 2020. The following sections discuss a literature review, methodology, data analysis, and the results.

Literature Review

Overview of Cybercrime

In the last 30 years, new technological platforms emerged to transform the way we operate almost all aspects of our lives. Unfortunately, these same technological advancements have also created new and relatively easier avenues for criminals to victimize people, organizations, governments, and businesses. Cybercrime is a term used to encompass a multitude of these new crimes which utilize the computer as a harmful weapon. There are many types of cybercrime which can range from identity theft (Holt & Turner, 2012), phishing (Ghazi-Tehrani & Pontell, 2021), cyberbullying (Whittaker & Kowalski, 2015), cyberfraud (Drew & Farrell, 2018), and cyberstalking (Reyns et al., 2011), to hacking (Marcum et al., 2014), data theft (Clough, 2011), malware attacks (Jansen & Leukfeldt, 2016), and cyberterrorism (Jarvis & Macdonald, 2015).

In physical crimes, for an incident to occur, generally the offender and victim must be in the same physical space. However, in the commission of cybercrime, the common link is not sharing a physical space, but instead sharing a virtual online space, with computers linked together. That means as offenders and victims increase in the online space, we would expect online crimes to increase, as well. As discussed in this section, the COVID-19 pandemic set up an ideal scenario for a large increase of offenders and victims sharing the same online space, which theoretically would lead to an increase in cybercrime.

Background of COVID-19 Pandemic

The COVID-19 pandemic greatly impacted the lives of Americans. The fast-moving pace of society quickly came to a halt as the U.S. government enacted mandatory stay-at-home orders across the nation. Roads emptied as non-essential businesses and schools shut down. Moreover, even more computers and tablets turned on as the world shifted to cyberspace. The general public watched the rising positive cases and death tolls each day, in which they wondered when society would return to normalcy. Some states, such as California, Florida, and Texas, accumulated over half a million reported positive COVID-19 cases from January to mid-August 2020 alone (Center for Disease Control [CDC], 2021a). In the first few months of the pandemic, these states' death rates each totaled almost 10,000, respectively. Both positive cases and death tolls have continued to increase rapidly since the onset of the virus.

As the COVID-19 pandemic attracted nationwide attention in the early months of 2020, state governors issued numerous public orders. On February 29, 2020, Washington declared a state of emergency, and all 50 states shut down by March 16, 2020 (Raifman et al., 2020). Subsequently, non-essential businesses (i.e., gyms, movie theaters, hair and nail salons, sporting event venues, etc.), and K-12 public schools, closed in mid-to-late March. Most states then issued mandatory stay-at-home orders in the last few days of March 2020 and the first week of April. By early April, new positive cases across the nation reached between 20,000 to 42,000 each day, while death tolls reached between 900 to 3,000 daily (CDC, 2021a). The number of positive COVID-19 cases remained consistent in the 20,000 range throughout April and into early May; however, there was a slight decrease in death tolls at this time. Most U.S. states responded to these reports by discontinuing or loosening the stay-at-home restrictions near mid-May and early June (Raifman, 2020).

COVID-19 Pandemic and Crime. In addition to the effect on American society, the COVID-19 pandemic has considerably altered crime. The pandemic has reduced the number of opportunities for criminals to commit conventional types of crimes. For example, minor group offenses decreased, likely attributed to the COVID-19 mandatory lockdowns and stay-at-home orders eliminating deviant peer groups from congregating (Boman & Gallupe, 2020). Moreover, property crimes (i.e., larceny and residential burglary) significantly dropped in March and April of 2020 (Jackman, 2020). With more individuals at home during the early months of the COVID-19 pandemic, criminals may have felt more reluctant to burglarize homes. Interestingly, some crimes, such as vehicle theft, did not have consistent findings across multiple cities (Ashby, 2020). However, the COVID-19 pandemic has simultaneously created new opportunities for crime. For example, business burglaries dramatically increased during the pandemic (Jackman, 2020). Instead of burglarizing homes, criminals may have felt more inclined to burglarize businesses that have closed due to the pandemic. Furthermore, crimes committed alone (i.e., intimate partner violence [IPV] and homicide) have also increased, presumably caused by the proximity to and lack of time away from cohabitants which could lead to violent altercations (Boman & Gallupe, 2020; Piquero et al., 2021). Although IPV increased during the pandemic, the actual increase may be more significant since most incidents go unreported.

The COVID-19 pandemic has also influenced cybercrime around the world. With the increased use of technology and computers, individuals can efficiently utilize cyberspace to engage in criminal activities. Cybercriminals are specifically utilizing the wavering atmosphere of the COVID-19 pandemic to victimize. These individuals incorporate various emotional appeals regarding the virus into their schemes to establish trust and eventually manipulate victims (Naidoo, 2020). Regarding types of cybercrime, phishing and malware infections are the two most commonly used during the pandemic worldwide (Lallie et al., 2020).

Phishing entails illegitimate parties inducing individuals to perform specific actions, such as sharing information or clicking on a link (Lallie et al., 2019). Phishing was prominent in 86% of the global attacks, while malware infections increased and were involved in 65% (Lallie et al., 2020). Furthermore, in the United Kingdom specifically, cybercrime and online fraud increased during the COVID-19 pandemic, along with higher rates of cybercrime in months with the strictest lockdown policies (Buil-Gil et al., 2020). Results of a survey also showed a significant increase in cybervictimization during the pandemic (Kashif et al., 2020). However, some research in the United States found no increase in cybercrime victimization, as well as no change in cyber routines (Hawdon et al., 2020). In this regard, the current study expects to contribute significant information to the impact of the COVID-19 pandemic on cybercrime victimization. The next section will explore the theoretical framework used to understand how COVID-19 may impact malware infections.

Routine Activities Theory

The Routine Activities Theory (RAT) is a commonly used criminology and victimization theory that explains the requisites for a crime to be committed. The theory consists of three components: a motivated offender, a suitable target, and the absence of capable guardians (Cohen & Felson, 1979). The theory explains that if any one of these crucial elements is not present, then the likelihood of a crime occurring decreases. Conversely, when situations arise when the convergence of these three elements occurs more often, crime is likely to increase. While initially used to describe traditional crime, RAT has now extended to cybercrime as well.

Motivated Offender. A motivated offender is necessary for a crime to transpire. Individuals utilize the Internet for many reasons, whether for e-mailing, searching the web, gaming, or shopping. These ordinary computer uses can later evolve into deviant activity and crime. As the number of Internet users increases, individuals have more potential to become offenders of cybercrime. According to one study, cybercrime offenders tend to be white males, with an average age of 38.2 years (Harbinson & Selzer, 2019).

Suitable Target. RAT requires a suitable target for the motivated offender to victimize. Any person is at risk for victimization, but offenders tend to target easy and vulnerable victims. Individuals who engage in risky online behaviors have an increased vulnerability to victimization and thus construct themselves as suitable targets (Reyns & Randa, 2020). Much like motivated offenders, increased Internet use in general may also create a more significant number of suitable targets (Ngo et al., 2020).

Absence of Capable Guardians. Traditionally, a capable guardian is a person or element that prevents a crime from taking place, such as police officers, security guards, parents, or street lighting (Cohen & Felson, 1979). However, after the emergence of cybercrime, these guardians can also take the form of antivirus protection or software, for example. Still, capable guardians are repeatedly absent from cyberspace, as they are often temporary, anonymous, and unable to intervene (Hawdon et al., 2019).

Online Exposure to Malware Infections. Numerous factors exist that expose individuals to cybercrime, specifically malware infections. Demographic predictors for victimization include unemployed younger males who live independently from their parents and have a less active offline social life (Näsi et al., 2015). Bergmann et al. (2018) also found that males and minors had an increased risk for victimization. Moreover, a better economic situation is associated with a lower risk of cybercrime victimization, especially from malware infections (Bergmann et al., 2018). Computer use and abilities may also contribute to

victimization. Akdemir and Lawless (2020) identified public computer use and insecure Wi-Fi connections as risk factors for malware infection victimization. In addition, a lack of knowledge and carelessness or inability to identify malware increased one's vulnerability (Kumar et al., 2018).

Interestingly, personality can be a factor in cybercrime victimization. In using traits from the Big Five model of personality, Van de Weijer and Leukfeldt (2017) reported that more open individuals were at a higher risk for victimization; however, those who were high in conscientiousness and emotional stability had a lower risk. Furthermore, individuals with lower self-control have an increased likelihood of experiencing malware infection indicators (Holt et al., 2020). Impulsivity may also increase proximity to malware, as these individuals may fail to utilize guardianship tools when exposed to a risky situation.

Research on Routine Activities Theory and COVID-19 Pandemic

Researchers of cybercrime and crime victimization, especially for malware infections, often use routine activities theory. A recent study discovered that motivated offenders have increased in the pandemic (Hawdon et al., 2020). This idea is consistent with the belief that more individuals are online due to the policies and practices necessitated by the COVID-19 epidemic. Unemployment due to COVID-19 is another factor that could increase the number of motivated offenders. In April 2020, the unemployment rate skyrocketed to 14.8% as the virus began to spread globally (Congressional Research Service [CRS], 2021). In addition, every state by April reached higher rates of unemployment than those during the Great Recession from 2007-2009. Unemployment could lead to a heightened need for money and a greater motivation to steal (Hawdon et al., 2019). Unemployment may motivate offenders to commit a crime, or unemployed individuals tend to spend more time on the Internet in general (Kigerl, 2012).

As for suitable targets, many studies have discovered numerous computer activities that increase the risk for cybervictimization, some of which are considered deviant. Ngo and colleagues (2020) found that greater online frequency led to higher cybervictimization. Bossler and Holt (2009) found that individuals, particularly those college-aged, who engaged in media piracy and viewed pornography were at a higher risk for malware infections. Furthermore, accessing government websites and engaging in online deviant activity (i.e., free streaming and peer-to-peer sharing) have been identified as risk factors for malware infection (Akdemir & Lawless, 2020). Other non-deviant computer activities that increased malware victimization risk include watching movies and visiting dating websites (Holt et al., 2020).

As for capable guardians, researchers have conducted substantial experimentation on the use of antivirus software and firewalls and their effect on cybervictimization. Bossler and Holt (2009) reported that software specifically designed to protect against malware infections had no impact on victimization. Later, Holt and Bossler (2013) found that individuals with antivirus software reported higher indicators of malware infections, and those with a hardwire firewall reported fewer. Moreover, Akdemir and Lawless (2020) found that the installation of antivirus software increased the risk for cybercrime victimization.

Additionally, crime opportunity theory (Felson & Clarke, 1998) suggests that criminal acts are highly determinant on criminal opportunities that present themselves to motivated offenders. As more people

were forced to spend time online during the pandemic for socialization, education, and business, the opportunities for motivated offenders to victimize online users also greatly increased. Furthermore, some schools, businesses, and organizations were forced to quickly and hastily shift operations to an online platform, without taking the time to adequately set up and implement proper cybersecurity measures, which also provided greater opportunities for cybercriminals.

Recent literature has examined the impact of COVID-19 on some types of cybercrime victimization; however, this is the first study to empirically test the relationship between COVID-19 and malware attacks on a national scale. Therefore, our study is a valuable addition to the literature on COVID-19 and cybercrime and, more largely, on COVID-19's impact overall on crime. This study will examine the relationship between COVID-19 positive cases, COVID-19-related lockdowns, and the number of malware attacks in the United States.

Current Study

The onset of the COVID-19 pandemic has necessitated new research on cybercrime. The virus's unprecedented practices and policies have undoubtedly changed the world of cybercrime and impacted victimization as a whole. Generally, one of the most prominent effects of the COVID-19 pandemic has been the closure of non-essential businesses and K-12 public schools. Moreover, high numbers of positive COVID-19 case numbers have led to more individuals staying at home, which in turn creates a larger online presence and greater chances for victimization. However, there is limited research on the relationship between malware infections specifically and closed non-essential businesses and K-12 public schools, as well as daily COVID-19 positive case numbers. Therefore, we hypothesize the following relationships:

H1: There is a positive relationship between closed non-essential businesses and malware infections in the U.S.
H2: There is a positive relationship between closed K-12 public schools and malware infections in the U.S.
H3: There is a positive relationship between daily COVID-19 positive numbers and malware infections in the U.S.

Methods

Data

Data utilized in this study derives from the Kaspersky Cyberthreat Real-Time Map and the Centers for Disease Control and Prevention (CDC) over the course of six months from January of 2020 to June of 2020. The Kaspersky Cyberthreat Real-Time Map was provided by Kaspersky Lab, an organization dedicated to cybersecurity and fighting cybercrime and cyberthreats (Kaspersky Lab). The daily numbers of malware infections were also collected from Kaspersky Lab. The CDC is an organization committed to protecting the safety and health of American citizens (CDC, 2021b). The CDC provided data on reported COVID-19 positive cases. In addition, the data for closed non-essential businesses and closed K-12 public schools was derived from the COVID-19 U.S. State Policy Database. This database includes state policies on closures, shelter-in-place orders, housing protections, changes to Medicaid, physical distancing closures, reopenings, and K-12 public school closings. In this regard, researchers at the Boston University School of Public Health

have visited state government websites to make the policy database as complete and accurate as possible in a rapidly changing policy context.

Measures

Dependent variable. A dependent variable for cybercrime victimization was measured by the number of malware infections in the United States per day. The number of malware infections in the U.S. ranged from 282,515 to 389,456 daily during the study's time frame.

Independent variables. Three items were gathered for the independent variables: COVID-19 positive cases, closed non-essential businesses, and closed K-12 public schools. The number of reported COVID-19 positive cases in the U.S. ranged from zero to 44,783 daily. The variable of closed non-essential businesses was dichotomously coded (0 indicating opened non-essential businesses; 1 indicating closed non-essential businesses). At the same token, the variable of closed K-12 public schools was dichotomously coded (0 indicating opened non-essential businesses; 1 indicating closed non-essential businesses).

Analytic Method

All models were estimated using SPSS 27. First, a correlation matrix was provided to show bivariate relationships between variables. Second, a series of Ordinary Least Squares (OLS) regressions were employed in order to test hypotheses 1-3 concerning the association between closed non-essential businesses, closed K-12 public schools, COVID-19 positive cases, and malware infection numbers. The OLS regression models were suitable to analyze this data since the relationship between the independent variables and dependent variable were linear. The Shapiro-Wilk test and Kolmogorov-Smirnov Test (K-S Test) determined that the dependent variable (see Flatt & Jacobs, 2019) was normally distributed (Shapiro-Wilk test: $p > .05$; 1-Sample Kolmogorov-Smirnov Test: $p > .05$). In addition, all the tolerance values are over .20 and all the VIF statistics are less than 10; therefore, there is no problem with multicollinearity among variables. The analyses began with a bivariate regression where closed non-essential businesses are modeled as the sole predictor of malware infection in order to obtain a baseline association. Next, closed K-12 public schools and COVID-19 positive case variables were added to the model.

Results

Table 1 provides descriptive statistics for the variables used in this study. The means for malware infection and COVID-19 positive case numbers were respectively 330,007 and 14,437; SD for both these variables were respectively 22,609 and 13,841. Prevalence rates for closed non-essential businesses was 18% (33 days out of 182 days). Prevalence rates for closed K-12 public schools was 41.2% (75 days out of 182 days).

Bivariate Relationships

Table 2 shows the bivariate correlations of the study variables. Both (1) closed non-essential businesses and (2) closed K-12 public schools had positive relationships with malware infection numbers. Also, COVID-19 positive cases had a positive relationship with malware infection numbers. In line with these results, our three hypotheses have been tested with one ordinary least squares (OLS) regression equation as below.

Table 1. *Cronbach's Alpha Coefficient for Reliability Analysis*

Variables	Mean	SD	Min	Max
Malware Infection	330007.10	22609.57	282515	389456
Closed Non-essential Business	.18	.38	0	1
Open (81.95%)				
Closed (18.1%)				
Closed K-12	.41	.49	0	1
Open (58.8%)				
Closed (41.2%)				
COVID-19 Reported Positive Cases	14437.14	13841.51	0	44783

Regression Analyses

Table 3 presents the results of the series of ordinary least squares (OLS) regressions analysis conducted in order to investigate the hypotheses. Model 1 indicates that there is a statistically significant, positive relationship between closed non-essential businesses and malware infection victimization (b = 13616.51, SE = 4253.22, β = .23, p < .01). This result indicates that closed non-essential businesses in the United States is positively associated with U.S. malware infection numbers which is the predicted direction of hypothesis 1. This result simply means that more closed non-essential businesses were related to higher malware infections. Model 2 adds two variables to account for differences in closed K-12 public schools. As shown, the COVID-19 positive numbers (b = .45, SE = .23, β = .27, p < .05) variable is a statistically significant predictor of malware infection number; moreover, the effect of closed non-essential business remains statistically significant (b = 19884.92, SE = 4475.09, β = .34, p < .001). However, the closed K-12 (b = 2344.62, SE = 6816.48, ß = .05, p > .05) variable is not a statistically significant predictor of malware infection number. In summary, these results reveal that closed non-essential businesses and COVID-19 positive case numbers have been influenced by the increasing likelihood of malware infection victimization, whereas closed K-12 schools were not associated with the likelihood of malware infection victimization. Given that, the findings of this study support hypotheses 1 and 3.

Table 2. *Correlations of the Study Variables*

	1	2	3	4
1. Malware Infection	1			
2. Closed Non-essential Business	.23**	1		
3. Closed K-12	.15**	-.39**	1	
4. COVID-19 Reported Positive Cases	.21**	.29**	-.87**	1

Notes. * p<.05, ** p<.01

Table 3. *Ordinary Least Squares (OLS) Results of Predicting Malware Infection Number (N=182)*

	Model 1			Model 2		
Variables	*b*		SE	*B*		SE
Closed Non-essential Business	13616.51***	2	4253.2	1988.92***	***9	4475.0
Closed K-12				2344.62	8	6816.4
COVID-19 Reported Positive Cases				.45*	.23	
R^2		.05			.15	

Notes. * $p<.05$, ** $p<.01$, ***$p<.001$

Discussion

This study sought to empirically investigate the relationship between malware infections, COVID-19 reported positive cases, closed non-essential businesses, and closed K-12 public schools in the United States. We hypothesized that the three independent variables, COVID-19 positive case numbers, closed non-essential businesses, and closed K-12 public schools would each have a positive relationship with malware infections. We assumed that the lockdowns and mandatory stay-at-home orders necessitated by the pandemic would increase the likelihood of malware infections because of increased Internet use. The results of this study indicate that there is a positive relationship between malware infections and COVID-19 positive cases, as well as a positive relationship with closed non-essential businesses. However, based on our findings, there is no relationship between malware infections and closed K-12 public schools. And, although not a focus of our study, another interesting finding was that COVID-19 positive cases were negatively related to closed K-12 public schools.

While some early research has shown that many types of physical crime decreased during the first few months of the pandemic (Abrams, 2021; Boman & Gallupe, 2020; Jackman, 2020), on the contrary, other studies have found an increase in cybercrime during the same period (Buil-Gil et al., 2020; Kashif et al., 2020; Lallie et al., 2020; Naidoo, 2020). Overall, our findings fall in line with these previous studies.

This study gives contradictory results to the research by Hawdon and colleagues (2020); however, this could be the result of the data utilized. Hawdon et al. (2020) used data from surveys given in November 2019 and April 2020 asking respondents if they had been cyber victims, then compared results before and after the pandemic and found no significant change. However, it is possible some users are not aware of cybervictimization, and the sample size was relatively small at 1000-1200 respondents. This study used a much larger dataset that measured actual cyberattacks happening in real-time in the United States, which could possibly be a more valid measure of cybercrime and could explain the different findings.

As a result of the COVID-19 pandemic, many activities of non-essential businesses and K-12 public schools moved from physical space to cyberspace. K-12 public schools utilized online learning systems, such as Google Classroom, Zoom, and Blackboard, to continue teaching and learning through the pandemic. We believe these safe spaces used by students and teachers may have influenced the lower risk of victimization.

Furthermore, past research has indicated that deviant computer activity increases the risk for victimization. Therefore, adult individuals employed by closed non-essential businesses may have engaged in these types of acts, escalating their likelihood of victimization.

As the emerging field of cybercrime significantly grows in the United States, there must be increased interest and concern regarding cybercrime prevention. The findings demonstrate a need to strengthen cybersecurity to eliminate threats and victimization. Our society might not have had enough cybersecurity countermeasures to protect our virtual communities against maliciously motivated cybercriminals at the beginning of the COVID-19 pandemic. It is also likely that many individuals were generally unprepared for the sudden shift from physical space to cyberspace. Therefore, society must take specific countermeasures to protect ourselves against cybercriminals. First, researchers in the field must continue to explore the strategies and techniques used by cybercriminals and share this information, especially with frequent Internet users. Individuals and companies then must familiarize themselves and recognize common types of cybercrime and the schemes often used by cybercriminals. The findings of the current study demonstrate the need to educate all individuals on cybersecurity and cybervictimization, as well as increase cybercrime awareness as a whole. Heightened alertness and better recognition of the various types of cybercrime will prove beneficial to those with high risks for victimization.

As mentioned earlier, since the onset of the pandemic, cybercriminals are integrating emotional appeals concerning the COVID-19 virus into their schemes (Naidoo, 2020). Given that, society must understand how a cybercriminal may use extraordinary or unexpected events, such as a global pandemic, to successfully carry out their crimes. As shown through the findings of the present study, the COVID-19 pandemic had a significant impact on cybercrime, especially malware infections. Nevertheless, when the pandemic presumably concludes, cybercriminals will simply find another relevant national or global event to incorporate into their schemes. Thus, the threat of cybercrime will likely never disappear, and society must continue to develop new and effective countermeasures against cybercriminals.

Furthermore, the onset of the virus magnified the use of computers and the Internet, creating more cybercriminal opportunities. The pandemic also caused work, school, and other social events to switch to cyberspace for an extended time and enabled individuals to become accustomed to completing various activities through cyberspace (i.e., food shopping, doctor appointments, fitness classes, etc.) Therefore, the world will become more dependent on the cyberworld than ever before, and we must direct our attention towards eliminating crime committed through cyberspace.

Although this study provides significant results on the relationship between malware infections and several aspects of the COVID-19 pandemic (reported positive cases, closed non-essential businesses, and closed K-12 public schools), the study has limitations that must be discussed. First, the dichotomous measure of closed/non-closed may not capture the full picture, as it is possible some businesses and schools were partially open and that was not indicated in the data. Also, this study utilized data from a period of six months, from January 2020 to June 2020; however, the COVID-19 pandemic did not directly affect the United States until early March of 2020. The first three months (January – March 2020) may then differ greatly from the second three months (April – June 2020). Therefore, future studies can compare various timeframes from throughout the pandemic to more closely investigate how and when the pandemic changed cybercrime. Moreover, future research can be directed towards the later months of 2020 and through 2021.

The current study does provide a correlational investigation, but does not address causation, therefore, future researchers also can utilize a before/after longitudinal study that further investigates the relationship between these variables. Lastly, this study focused entirely on malware infections. Future studies can focus on other types of cybercrime to explore if there are similar relationships with the three independent variables used in this study.

Conclusion and Implications

The onset of the COVID-19 pandemic radically changed the physical and cyberworlds and the criminal activity that occurs within. This study sought to empirically investigate how the societal changes brought about by the pandemic affected malware infections specifically. The results indicate a positive relationship between malware infections and closed non-essential businesses and between malware infections and reported COVID-19 positive cases. Interestingly, there is no relationship between malware infections and closed K-12 public schools.

The findings of the study demonstrate many implications. First, there is a need to continue research that investigates the global pandemic and its effects on both the physical and virtual worlds. The findings also strongly suggest a need for increased cybervictimization awareness as the threat of cybercrime intensifies and the COVID-19 pandemic continues. However, following the end of the pandemic, we must still recognize the danger and risks of cybercrime and the threat it will continue to impose as technology advances and cybercriminals adapt. Furthermore, the current study has shown how the COVID-19 pandemic, a significant and extraordinary world event, has exceptionally altered cybercrime. Therefore, we must note that these types of circumstances may trigger sudden changes in cybercrime and victimization. When these events occur, we must take precautions and sense how it could bring changes to the physical and cyber worlds. Importantly, through the present study, we have directly witnessed how the COVID-19 pandemic has transformed our lives in the physical and virtual realms.

References

Abrams, D. S. (2021). COVID and crime: An early empirical look. *Journal of Public Economics, 194,* 104344.

Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: a lifestyle routine activities approach. *Internet Research, 30(6)*, 1665-1687.

Ashby, M. P. (2020). Initial evidence on the relationship between the coronavirus pandemic and crime in the United States. *Crime Science, 9*(1), 1-16.

Bergmann, M. C., Dreißigacker, A., von Skarczinski, B., & Wollinger, G. R. (2018). Cyber-dependent crime victimization: the same risk for everyone?. *Cyberpsychology, Behavior, and Social Networking, 21*(2), 84-90.

Boman, J. H., & Gallupe, O. (2020). Has COVID-19 changed crime? Crime rates in the United States during the pandemic. *American Journal of Criminal Justice, 45*(4), 537-545.

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology, 3*(1), 400-420.

Brynjolfsson, E., Horton, J. J., Ozimek, A., Rock, D., Sharma, G., & TuYe, H. Y. (2020). *COVID-19 and remote work: An early look at US data (No. w27344).* National Bureau of Economic Research.

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2020). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies, 23*(1), 47-59.

Center for Disease Control [CDC]. (2021a). *Compare Trends in COVID-19 Cases and Deaths in the US.* COVID Data Tracker. https://covid.cdc.gov/covid-data-tracker/#compare-trends_totalcases

Center for Disease Control [CDC]. (2021b). *About CDC 24-7: A Bold Promise to the Nation.* https://www.cdc.gov/about/24-7/index.html

Clough, J. (2011). Data theft? Cybercrime and the increasing criminalization of access to data. *Criminal Law Forum, 22*, 145-170.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-608.

Congressional Research Service [CRS]. (2021, January 12). *Unemployment Rates During the COVID-19 Pandemic: In Brief.* https://fas.org/sgp/crs/misc/R46554.pdf

Drew, J. M., & Farrell, L. (2018). Online victimization risk and self-protective strategies: Developing police-led cyber fraud prevention programs. *Police Practice and Research, 19*(6), 537-549.

Felson, M., & Clarke, R. V. (1998). Opportunity makes the thief. *Police Research Series, Paper 98*(1-36), 10.

Ghazi-Tehrani, A. K., & Pontell, H. N. (2021). Phishing evolves: Analyzing the enduring cybercrime. *Victims & Offenders, 16*(3), 316-342.

Harbinson, E., & Selzer, N. (2019). The risk and needs of cyber-dependent offenders sentenced in the United States. *Journal of Crime and Justice, 42*(5), 582-598.

Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amid COVID-19: The Initial Results from a Natural Experiment. *American Journal of Criminal Justice, 45*(4), 546-562.

Holt, T. J., & Bossler, A. M. (2013). Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice, 29*(4), 420-436.

Holt, T. J., van Wilsem, J., van de Weijer, S., & Leukfeldt, R. (2020). Testing an integrated self-control and routine activities framework to examine malware infection victimization. *Social Science Computer Review, 38*(2), 187-206.

Holt, T. J., & Turner, M. G. (2012). Examining risks and protective factors of on-line identity theft. *Deviant Behavior, 33*(4), 308-323.

Internet Crime Complaint Center. (2019). *2019 Internet Crime Report.* Federal Bureau of Investigation. https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf

Jackman, T. (2020, May 19). *Amid pandemic, crime dropped in many U.S. cities, but not all.* The Washington Post. https://www.washingtonpost.com/crime-law/2020/05/19/amid-pandemic-crime-dropped-many-us-cities-not-all/

Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology, 10*(1), 79.

Jarvis, L., & Macdonald, S. (2015). What is cyberterrorism? Findings from a survey of researchers. *Terrorism and Political Violence, 27*(4), 657-678.

Kashif, M., Javed, M. K., & Pandey, D. (2020). A surge in cyber-crime during COVID-19. *Indonesian Journal of Social and Environmental Issues (IJSEI), 1*(2), 48-52.

Kaspersky Lab. (n.d.). *About Us.* https://usa.kaspersky.com/about

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review, 30*(4), 470-486.

Kumar, A., Ojha, N., & Srivastava, N. K. (2018). Factors affecting malware attacks: An empirical analysis. *PURUSHARTHA-A Journal of Management, Ethics and Spirituality, 10*(2), 46-59.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2020). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security, 105,* 102248.

Marcum, C. D., Higgins, G. E., Ricketts, M. L., & Wolfe, S. E. (2014). Hacking in high school: Cybercrime perpetration by juveniles. *Deviant Behavior, 35*(7), 581-591.

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems, 29*(3), 306-321.

Näsi, M., Oksanen, A., Keipi, T., & Räsänen, P. (2015). Cybercrime victimization among young people: A multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention, 16*(2), 203-210.

Ngo, F. T., Piquero, A. R., LaPrade, J., & Duong, B. (2020). Victimization in cyberspace: Is it how long we spend online, what we do online, or what we post online?. *Criminal Justice Review, 45*(4), 430-451.

Piquero, A. R., Jennings, W.G., Jemison, E., Kaukinen, C., and Knaul, F.M. (2021). Domestic violence during COVID-19: Evidence from a systematic review and meta-analysis. *Journal of Criminal Justice (74)*, 101806.

Raifman, J., Nocka, K., Jones, D., Bor, J., Lipson, S., Jay, J., & Chan, P. (2020). COVID-19 U.S. state policy database. www.tinyurl.com/statepolicies

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior, 38*(11), 1149-1169.

Reyns, B. W., & Randa, R. (2020). No honor among thieves: personal and peer deviance as explanations of online identity fraud victimization. *Security Journal, 33*(2), 228-243.

Sabillon, R., Cano, J. J., Cavaller Reyes, V., & Serra Ruiz, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security, 4*(6).

Van de Weijer, S. G., & Leukfeldt, E. R. (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking, 20*(7), 407-412.

Whittaker, E., & Kowalski, R. M. (2015). Cyberbullying via social media. *Journal of School Violence, 14*(1), 11-29.